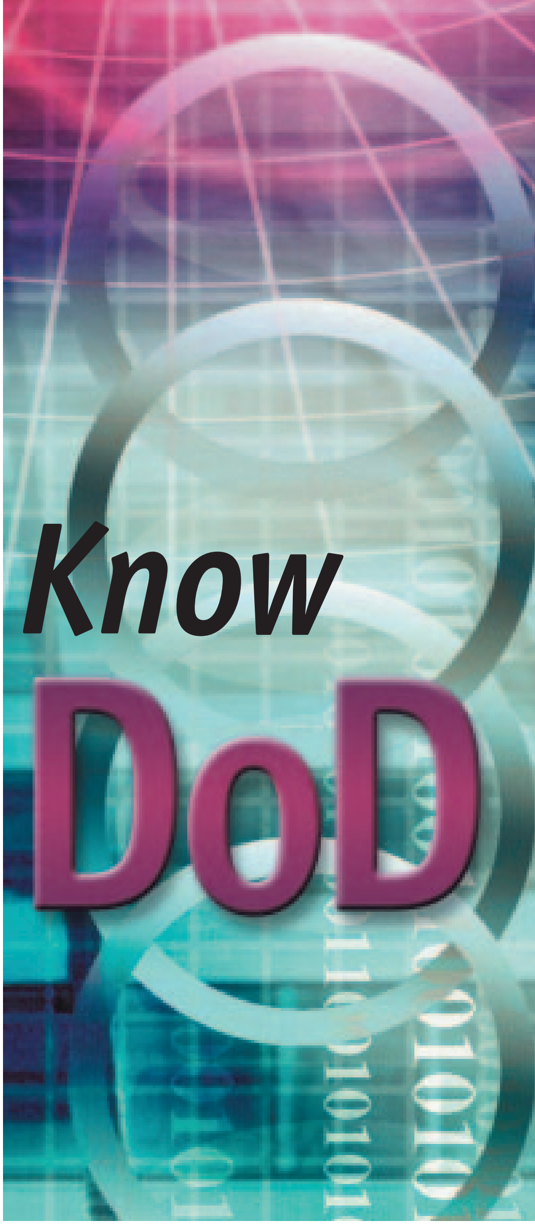
Julie Gable, CRM, CDIA

Everything You Wanted to Know About DoD



The standard is not a panacea or a guarantee, but it is a tangible contribution in a field hungry for guidance

At the Core

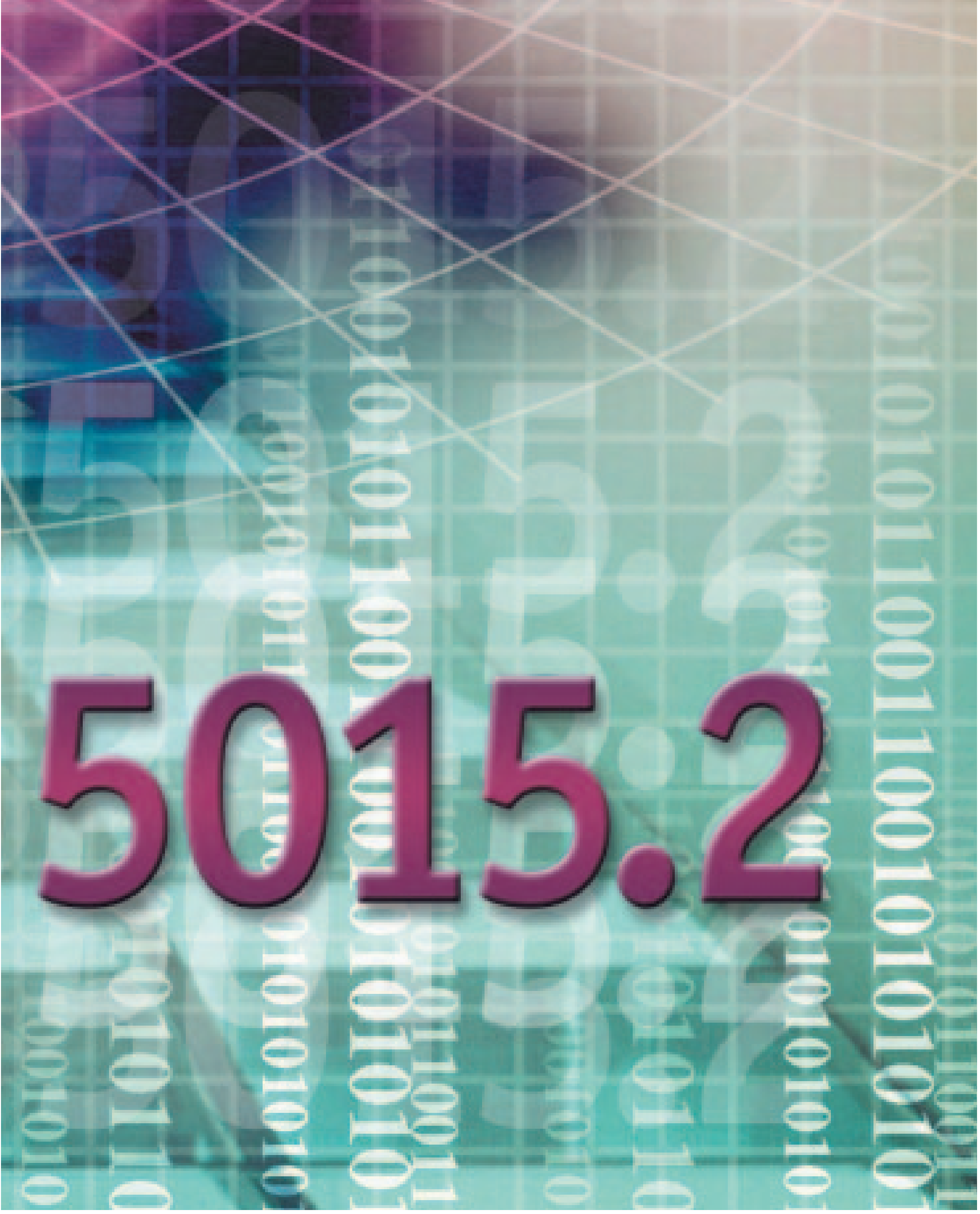
This article:

- Defines DoD 5015.2 and its requirements
- Explains the standard's certification process
- Analyzes strengths and weaknesses of the standard

The U.S. Department of Defense's (DoD) *Design Criteria Standard for Electronic Records Management Software Applications*, better known as DoD 5015.2, debuted in 1997. Since then, it has become a de-facto standard that government agencies, including the National Archives and Records Administration (NARA), readily endorse. Private sector businesses routinely use standard certification – or lack thereof – as a way to shortlist records management software for potential purchases. DoD 5015.2 is also the starting point for such benchmarks as the United Kingdom's Public Record Office (PRO) standard and the European Union's Model Requirements (MoReq).

Outside the DoD, however, the standard is not necessarily well understood. Ask attendees at any electronic records seminar whether they are aware of the standard and nearly all raise their hands. Ask whether they want software that is certified to the standard and, again, the majority assent. Ask how many have actually read the standard, however, and the percentage drops significantly. Given the short-staffed nature of most records programs and the subsequent time crunch it produces, such a response is understandable.

But is it realistic to assume that software configured to a federal department's specification applies just as well to commercial enterprises? More importantly, is it correct to assume that whatever software vendors develop to obtain certification automatically becomes part of their products? Does the dictum "Must be DoD 5015.2-certi-



fied" in a request for proposal shortcut the need for analyzing an organization's needs in more depth? Not all business customers require certification; not all software vendors seek it. Why?

The Standard Evolves

The standard's origins provide a partial answer and illustrate the key role that archival principles played in its evolution. In 1993, a DoD records management task force that included representatives from NARA, the U.S. Army, the U.S. Air Force, and the Army Research Laboratory began the work of re-engineering records management processes. In doing so, the task force considered research and theoretical constructs from the University of British Columbia and the University of Pittsburgh that focused on assuring the reliability and authenticity of electronic records. (See sidebar on page 36.)

Two years later, the task force published its findings in the report "Functional Baseline Requirements and Data Elements for Records Management Application Software." The report circulated to several federal and DoD agencies, as well as to software vendors, soliciting comment on the 47 requirements identified.

With the task force's charter fulfilled, the DoD turned to the Defense Information Systems Agency (DISA), the unit responsible for acquiring and managing shared office information systems, to continue the work. DISA relied on its testing and evaluation component, the Joint Interoperability Test Command (JITC), to clarify the report's requirements and establish a certification testing program.

"In 1996, Steve Matsuura, my boss at JITC, and I began to draft the standard," recalls Bill Manago, currently product manager for MDY Advanced Technologies, who was then in the armed forces. "We took into account NARA and other federal RM directives, incorporated research provided by Australian and Canadian standards, and developed requirements for managing e-mail as records." The result was DoD 5015.2, *Design Criteria Standard for Electronic Records Management Software Applications*. JITC remains responsible for maintaining the standard and administering the software certification testing program.

What the Standard Is

Revised in June 2002, the DoD 5015.2 standard defines mandatory functionality for records management application (RMA) software used within the DoD. Each mandatory functional requirement is included because it relates to U.S. federal regulation and/or NARA policy; these are listed in the standard document's references section. The standard's glossary of terms, as well as its list of acronyms and abbreviations, is useful for anyone not familiar with records management. Newly added to the June 2002 version is Chapter Four with requirements for records management applications supporting classified (i.e., secret) records. Other differences from the 1997 version include expanded requirements for audit, more functionality for user-defined metadata fields, and additional e-mail requirements.

Figures 1 and *2* list the requirements of 5015.2's 2002 version. Each mandatory requirement has several subparts, and each subpart specifies particular functionality. Required functionality reflects the way basic electronic recordkeeping practices work in government. This is important because such practices collectively form a model, a construct, for how the records management software must work. All records management software – whether for paper or electronic records, whether for DoD use or not – must be configured to mirror an organization's underlying

Figure 1: DoD 5015.2, June 2002 – Mandatory Elements

DoD 5015.2 Section	Element	Records Management Application Mandatory Functionality	Number of Sub parts
C2.1 General Requirements	C2.1.1	Manage records regardless of storage media	0
	C2.1.2	Accommodate four-digit dates	0
	C2.1.3	Add user-defined fields and change field labels	0
	C2.1.4.	Support backward compatibility with earlier product versions	0
	C2.1.5.	Comply with Americans with Disabilities Act requirements	0
	C2.2.1.	Implementing File Plans – Standard specifies mandatory file plan components and mandatory record folder components.	6
	C2.2.2	Scheduling Records	7
	C2.2.3.	Declaring and Filing Records – Standards specifies mandatory metadata requirements.	26
	C2.2.4.	Electronic Mail	3
	C.2.2.5.	Storing Records	4
	C2.2.6.1.	Screening Records (Life Cycle)	5
	C2.2.6.2.	Closing Record Folders (Life Cycle)	2
	C2.2.6.3.	Cutting Off Record Folders (Life Cycle)	2
	C2.2.6.4.	Freezing/Unfreezing Records (Life Cycle)	4
	C2.2.6.5.	Transferring Records (Life Cycle)	5
	C2.2.6.6.	Destroying Records (Life Cycle)	6
	C2.2.6.7.	Cycling Vital Records	4
	C2.2.6.8.	Searching for and Retrieving Records	9
	C2.2.7.	Access Controls	5
	C2.2.8	System Audits	6
	C2.2.9	System Management	6

model of recordkeeping practices in order to work at all. For example, are documents considered records at creation, at approval, or when submitted to an outside agency? Once documents are declared records, should they move from their creation repository to a "protected" repository with limited access? The answers may differ depending on the environment's rules and needs.

The DoD standard's underlying model reflects its government and archives roots. The federal government defines a record as any document that evidences an agency's performance of its mission, regardless of physical form or media – a broad definition whose interpretation could encompass nearly all documents. Federal agencies, therefore, must decide what is a record and what is not.

For records management software, the model assumes that document creators follow practices that dictate when documents become records. The model also makes creators responsible for classifying records in a folder hierarchy according to a well-understood, uniform filing plan.

The DoD standard, in fact, prescribes mandatory file plan components and mandatory record folder components, indicating required data collection by users. In the private sector, practices may be quite different. Corporate lawyers contend that everything is a record. Placing electronic records into a folder hierarchy is one way to attach retention rules to them, but it is not the only way. Information technology staff, for example, contends that designating documents as records should be automatic, based on underlying workflows.

The federal government must also preserve the public record for posterity, giving particular weight to concerns about records' authenticity and reliability in an electronic world. The standard requires transferring records with historic value to archival facilities, specifying that records should be copied with their associated metadata and their folders. The standard requires 16 mandatory metadata fields, though not all must be captured for each record type.

Archival Influences

The University of British Columbia's work emphasizes the reliability and authenticity of electronic records, using diplomatics as a basis. Diplomatics, which dates from the 17th century, establishes rules for determining whether a document is authentic and reliable based on particular characteristics. Adapting these principles to modern electronic recordkeeping, the university developed templates showing what elements are essential for records to be reliable and authentic. That work posits that all records, regardless of media, should be managed in the same way, that the recordkeeping rules must be embedded in the business process, and that the record's creator is responsible for the record's long-term authenticity and reliability. The work covers records' creation, use, and preservation, and implies the existence of a central control point to which responsibility can be transferred when the creator no longer needs the record.

The University of Pittsburgh's work asserts that an electronic record must be managed from the time it is created and emphasizes that electronic data may not be separable into life cycle stages. Pittsburgh's research gathered all known recordkeeping requirements, categorized them by type, then identified a software functionality that would achieve each type of requirement. Pittsburgh also posited that a record's value might be derived from where it is filed, a construct that assumes the existence of a file plan.

In her doctoral dissertation and a subsequent interview, Mary Rawlings-Milton of Millican and Associates pointed out that the standard imposes a burden on records kept for a short time: "Do you really need all that metadata for short-term records?" In her experience implementing records software at a government agency, she found that "you are actually balancing what the software will do and what people will do." In the private sector, automatic capture of metadata is emphasized, largely for retrieval purposes rather than archival needs.

The standard recognizes certain requirements as site-specific, such as those for storage management, system performance, user training, and so forth. Other useful features identified include report writing, global change, and online help, among others. While admittedly nice to have, these features cannot be made mandatory because there is no federal law or NARA policy that requires them.

The Certification Process

JITC uses 27 test cases to determine whether a RMA meets the DoD standard's mandatory requirements. One-third of cases require only information or documentation. For the remaining 18, software vendors prepare scripts showing step-by-step procedures and accompanying screen shots for performing the required function. Test scripts go to the JITC eight weeks in advance of testing. "The test scripts show that the software is finished prior to testing," explains Bruce Miller, president of Tarian Software. "It is a way to prove in advance that the software can pass." There is no testing for non-mandatory or useful features.

JITC personnel travel from Fort Huachuca, Arizona, to the vendor's site. Testing for new, uncertified products may require two weeks, while certifying new versions of previously certified products may take four or five days. Most vendors devote two full-time resources to the test to provide technical expertise for its duration. JITC test personnel, who are TRW-supplied contract employees with records and software experience, work through each test case hands-on, using the software and the vendor's scripts to perform the required functions. Tests are pass/fail, and RMAs must pass all tests covering mandatory requirements. Work-arounds developed to satisfy requirements are permitted, and it is common for software vendors to add functionality specifically to pass the test.

Product certification status is added to JITC's Web site within days following successful test completion. A summary report appears within two to three weeks, followed by a detailed report, "for official use," two or three months later. Only government entities have access to full-length reports because vendors expressed concern about competitor access to proprietary information. Detailed reports contain information regarding work-arounds and include commentary on the number of screens or mouse-clicks required to perform various tasks. Vendors receive all reports prior to publication to check for accuracy.

Certification lasts for two years. It is granted on a particular software version, so any new version also must undergo testing. In product pairings (e.g., RMA software integrated with a document management product), the certification applies only to the pairing – not to the individual products. Document management vendors who claim their product is DoD 5105.2 certi-

Figure 2: DoD 5015.2, June 2002 – Non-Mandatory and Useful Features

DoD 5015.2 Section	Element Number	Records Management Application Non-Mandatory Features To Be Defined by Acquiring or Using Activity
C3.1 Non-Mandatory Features	C3.1.1	Storage Availability
	C3.1.2	Documentation
	C3.1.3	System Performance
	C3.1.4	Hardware Environment
	C3.1.5	Operating System Environment
	C3.1.6	Network Environment
	C3.1.7	Protocols
	C3.1.8	Electronic Mail Interface
	C3.1.9	End User Orientation and Training
C3.2 Other Useful Features	C3.2.1	Making Global Changes
	C3.2.2	Bulk Loading Capability – for pre-existing file plans, electronic records, record metadata
	C3.3.3	Interfaces to Other Software Applications
	C3.2.4	Report Writer Capability
	C3.2.5	On-Line Help
	C3.2.6	Document Imaging Tools
	C3.2.7	Fax Integration Tools
	C3.2.8	Bar Code Systems – for non-electronic records
	C3.3.9	Retrieval Assistance (e.g., full text search)
	C3.2.10	File Plan Component Selection / Search Capability
	C3.2.11	Workflow and or Document Management Features
	C3.2.12	Records Management Forms and Other Forms – for NARA and government forms
	C3.2.13	Printed Labels
	C3.2.14	Viewer
	C3.2.15	Web Capability
	C3.2.16	Government Information Locator Service
	C3.2.17	Enhanced Support for Off-line Records

fied actually mean that it is certified as paired with a specific RMA product.

"Watch out for the phrase 'DoD compliant'," advises Steve Matsuura, senior electronic engineer who oversees the test process at JITC. "Some vendors who are not certified will use this term. Vendors can only say they are certified if their product has passed the testing process and is listed on the JITC Web site."

RMA software vendors pay JITC $20,000 to $22,000 for an initial certification test and about $10,000 to $15,000 for a re-certification or a product pairing. Vendors also pay JITC personnel's travel expenses. Add the cost of vendor software engineers involved in coding ($50 to $600 per day), to the time required for advance test preparation and the resources devoted to the testing process itself, and the cost to vendors is significant. If a product fails, it moves to the test schedule's end, a queue with a year's wait, because all products want to certify against the June 2002 standard.

Different Perspectives

Despite the expense, certification has value for vendors. "DoD certification has rapidly become a mandatory requirement for most sales," says Tower Software President Frank McGovern. "We have found that many of our commercial clients, particularly those in regulated industries, insist on DoD certification. Certification mitigates risk: nobody wins if the software pilot fails." Tarian's Miller concurs, "For the government market, no certification means no sales. In private industry, certification is a convenient moniker – a shorthand way of stating qualifications."

The Library of Virginia's Bob Nawrocki agrees. He must select software that will enable the library to archive electronic records from Virginia Governor Mark Warner and his cabinet. Nawrocki placed DoD 5015.2-certified software at the top of his list for consideration. "It is comforting to have an objective baseline that all ERM software products are measured against," he says. "It assures that products that pass the test criteria have a certain minimum functionality."

Few of the standard's underlying assumptions on recordkeeping may hold true for the private sector, however. Moving records from one repository into another – for example from a document management system's repository to a records management software's repository – is not desirable in some environments; classification within uniform hierarchies is perceived as undue user burden, particularly in cases where documents, slide presentations, Web sites, and the like are part of ongoing collaboration. An electronic records analyst at a large consumer products firm stated that the DoD 5015.2 standard did not figure in his firm's choice of an RM software product two years ago. “Government and business operate very differently,” he said. “The standard’s focus is primarily for the military; it has no real effect on us.”

Sylvia Diaz, director of Records and Literature Management at Bristol-Myers Squibb’s Pharmaceutical Research Institute, observes: “DoD 5015.2 dictates a certain level of validation and standardization for RMAs that otherwise many not be there. However, the standards imposed are not all relevant to the pharmaceutical industry. Therefore, in the choice of RMA software for us, the standard would not be relevant. RM system developers would be wise to adhere to regulations like 21 CFR Part 11 as well.”

Software vendors who target the private sector tell a similar story. According to one reliable industry source, “The standard hurts creativity by forcing all software to work the same way. It errs on the side of telling vendors how to accomplish a function, not just what software must do.”

Art Bellis of OmniRIM agrees. “DoD makes RM onerous. Business has internal goals and budgets, and generally can’t afford to layer on superfluous requirements.” He estimates that it would take 1.5 years and $350,000 just to code, let alone develop, a product to DoD specifications. “DoD is a good step in the right direction for bringing accountability, but it may be impractical for business,” he says.

Strengths and Weaknesses

Ironically, the standard was never intended to become an industry touchstone. JITC’s Matsuura notes that the standard’s influence in the marketplace actually complicates the certification process. “Certification is a test of basic functionality; it is intended to tell *what* a product must do, not specify *how* the product should do it,” he says. The JITC is careful not to dictate how systems should be implemented, as this has implications for competition within the software industry.

The standard’s military origin will continue to influence its future. Although the 1997 standard identified Freedom of Information Act (FOIA) requirements and privacy considerations as future directions, the need for classified information practices took precedence in the 2002 version. Funding for the 5015.2 program comes from Assistant Secretary of Defense Command Control Communications and Intelligence (ASDC3I), with JITC reporting to this function’s chief information officer. Defense-related recordkeeping needs will likely continue to take precedence.

Another consideration is that the test process does not measure system performance, for example, how quickly searches execute; nor does it measure scalability, the software’s ability to handle tens, hundreds, or thousands of users with equal ease. All tests are on criteria that can be objectively measured, so no judgments are made with regard to the software’s ease of use or intuitiveness, other than tallies of total clicks or screens shown in the detailed report. There are no measures for how well any software’s modules interact or how elegantly the underlying code is written. Though not as important to records and information managers, such data can be useful to the selecting organization’s information technology group.

Interoperability (i.e., the means for different RMAs to share data) is not part of the standard and is not tested. “Interoperability between RMAs requires technology specification,” explains Matsuura. “DoD does not want to specify technology.”

This may change in the future as the JITC continues its work with NARA on e-government initiatives addressing additional metadata for permanent e-records. Ideally, NARA wants all RMAs to create an upload file in a format that NARA systems could parse automatically as part of electronic records preservation efforts.

The DoD 5015.2 standard appeared while electronic recordkeeping techniques were in their infancy. It offers an objective test of basic functionality within prescribed conditions, with particular emphasis on authenticity and reliability of electronic records with archival value. Going forward, the standard will evolve to meet government’s changing needs. The JITC also reviews all comments and suggestions as a means for continuous improvement.

In the private sector, the standard offers a starting point, a certain assurance of basic functionality. By itself, it is not a substitute for understanding an organization’s practices, a panacea for technical ills, or a guarantee of successful software implementation. DoD 5015.2 is a tangible contribution in a field generally hungry for guidance. The help it provides is welcome and appreciated.

Julie Gable, CRM, CDIA, *is the Principal of Gable Consulting, the Associate Executive Editor of* The Information Management Journal, *and a contributing editor for* Transform *magazine. She may be contacted at* JulieGable@aol.com.

References

Mary Rawlings-Milton. “Electronic Records & The Law: Causing the Federal Records Program to Implode?” (Ph.D. diss., Virginia Polytechnic Institute and State University, 2000). Available at *http://schholar.lib.vt.edu/theses/available/etd-04202000-13400008/unrestricted/erecs.pdf* (accessed 14 October 2002).

Records Management Application Compliance Test and Evaluation Process and Procedures. September 2002. Available at *http://jitc.fhu.disa.mil/recmgt/* (accessed 14 October 2002).

Design Criteria Standard for Electronic Records Management Software Applications. Available at *http://jitc.fhu.disa.mil/recmgt/* (accessed 14 October 2002).

DoD 5015.2-STD RMA Compliance Test Procedures. Version 6.5. September 2002. Available at *http://jitc.fhu.disa.mil/recmgt/* (accessed 14 October 2002).